

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000357127 A**(43) Date of publication of application: **26.12.00**

(51) Int. Cl.

G06F 12/14(21) Application number: **11170189**(22) Date of filing: **16.06.99**(71) Applicant: **TOSHIBA CORP**

(72) Inventor: **KAMIBAYASHI TATSU
YAMADA HISASHI
WASAKI HIROSHI
TAMURA MASABUMI
ISHIBASHI YASUHIRO
KATO HIROSHI
TOMA HIDEYUKI**

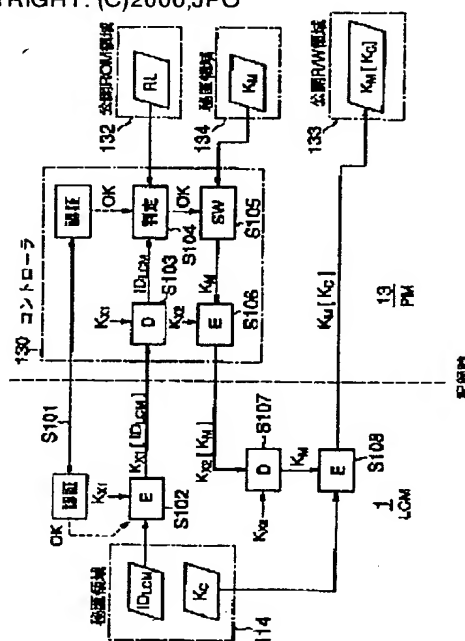
(54) **STORAGE MEDIUM AND COSNTENTS
MANAGING METHOD USING THE MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To surely detect and make ineffective a device which has a problem and to use discrimination information characteristic of an unusable storage medium to cipher or decipher contents or a contents key when a device which is not made ineffective is made ineffective.

SOLUTION: In an open ROM area 132 secured on a PM (storage medium) 13, a revocation list RL is previously registered and when the PM 13 is used to record contents by, for example, an LCM (contents use management system) 1, a controller 130 of the PM 13 receives discrimination information IDLCM (ciphered information of which) of the LCM 1, refers to the list RL according to the information, and decides whether or not the LCM 1 is made ineffective according to the reference result. Only when it is decided that the LCM is not made ineffective, a media key KM made secret in a secret area 134 is (ciphered and) passed to the LCM 1 and used to cipher the contents key KC.

COPYRIGHT: (C)2000,JPO



特開2000-357127

(P2000-357127A)

(43) 公開日 平成12年12月26日(2000.12.26)

(51)Int. Cl. 7

識別記号

F I

フォーマット(参考)

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 F

5B017

3 2 0 B

審査請求

未請求

請求項の数 10

O L

(全 14 頁)

(21) 出願番号 特願平11-170189

(22) 出願日 平成11年6月16日(1999.6.16)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 上林 達

神奈川県川崎市幸区小向東芝町1番地

株式会社東芝研究開発センター内

(72) 発明者 山田 尚志

東京都港区芝浦一丁目1番1号

芝本社事務所内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

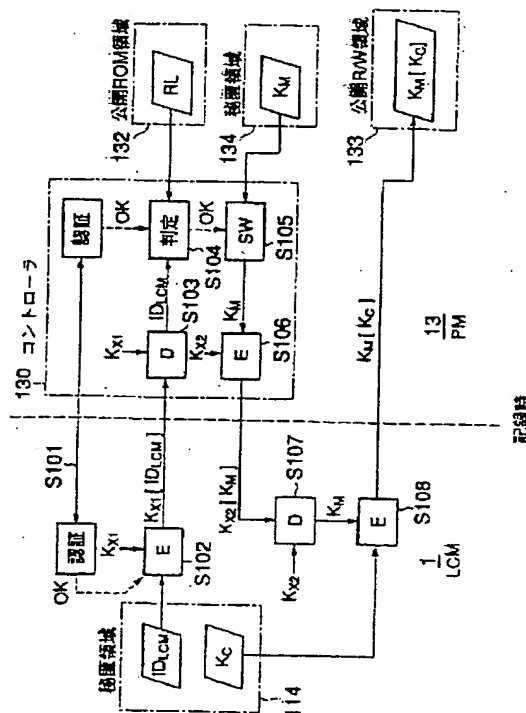
最終頁に続く

(54)【発明の名称】記憶媒体及び同媒体を使用したコンテンツ管理方法

(57)【要約】

【課題】問題のある機器を確実に検出して無効化し、無効化しない機器の場合、無効化されたならば利用不可能な記憶媒体に固有の識別情報をコンテンツまたはコンテンツキーの暗号化または復号化に用いさせることができるようにする。

【解決手段】PM(記憶媒体)13上に確保された公開ROM領域132に、リポケーションリストRLを予め登録しておき、当該PM13が例えばLCM(コンテンツ利用管理システム)1によるコンテンツの記録に用いられる場合に、PM13のコントローラ130が、LCM1の識別情報ID_{LCM}(の暗号化情報)を受け取って、その情報によりリストRLを参照し、その参照結果に応じてLCM1を無効化するか否かを判定する(ステップS104)。そして、無効化しないと判定した場合だけ、秘匿領域134に秘匿されているメディアキーK_Mを(暗号化して)LCM1に渡して、コンテンツキーK_Cの暗号化に用いさせる。



【特許請求の範囲】

【請求項 1】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された特定記憶領域と、

任意の電子機器による記録または再生に利用される場合に、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記リボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定する判定手段と、前記判定手段により無効化すべきでない判定された場合だけ、前記電子機器に対して自身に固有の秘匿されたメディア識別情報を渡して、そのメディア識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いさせる暗号化／復号化キー送出手段とを含むコントローラとを具備することを特徴とする記憶媒体。

【請求項 2】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が記憶される特定記憶領域と、リボケーション情報が付加されたデジタルコンテンツが電子機器により記録される際に、当該リボケーション情報により前記特定記憶領域上のリボケーション情報を更新する更新手段と、デジタルコンテンツが電子機器により記録される際と、前記記憶媒体に記録されたデジタルコンテンツが電子機器により利用される際には、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記特定記憶領域に記憶されているリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、その判定結果に応じて当該電子機器の無効化を制御する判定手段とを含むコントローラとを具備することを特徴とする記憶媒体。

【請求項 3】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なバージョン情報付きリボケーション情報が記憶される特定記憶領域と、

バージョン情報付きリボケーション情報が付加されたデジタルコンテンツが電子機器により記録される際に、当該リボケーション情報のバージョン情報と前記特定記憶領域に記憶されているリボケーション情報のバージョン情報とを比較し、その比較結果に基づいて前記特定記憶

領域に最新のリボケーション情報が記憶されるように更新制御する更新手段と、デジタルコンテンツが電子機器により記録される際と、前記記憶媒体に記録されたデジタルコンテンツが電子機器により利用される際には、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記特定記憶領域に記憶されているリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、その判定結果に応じて当該電子機器の無効化を制御する判定手段とを含むコントローラとを具備することを特徴とする記憶媒体。

【請求項 4】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なバージョン情報付きリボケーション情報が記憶される特定記憶領域と、

バージョン情報付きリボケーション情報が付加された暗号化デジタルコンテンツであって、当該リボケーション情報が前記コンテンツを復号するためのコンテンツキーと合わせてシステムに共通のマスタキーにより暗号化された暗号化デジタルコンテンツが電子機器により記録される際に、当該リボケーション情報のバージョン情報と前記特定記憶領域に記憶されているリボケーション情報のバージョン情報とを比較し、その比較結果に基づいて前記特定記憶領域に最新のリボケーション情報が記憶されるように更新制御する更新手段と、暗号化デジタルコンテンツが電子機器により記録される際と、前記記憶媒体に記録された暗号化デジタルコンテンツが電子機器により利用される際には、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記特定記憶領域に記憶されているリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、その判定結果に応じて当該電子機器の無効化を制御する判定手段と、前記記憶媒体に記録された暗号化デジタルコンテンツが電子機器により利用される際は、前記判定手段により無効化すべきでない判定された場合だけ、当該電子機器に対して秘匿された前記マスタキーを渡して、そのマスタキーをコンテンツ復号用のコンテンツキーの復号化に用いさせるマスタキー送出手段とを含むコントローラとを具備することを特徴とする記憶媒体。

【請求項 5】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体部とコントローラとが一体化された記憶媒体に特定記憶領域を設けて、当該特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報を予め登録しておく、

前記記憶媒体の1つが任意の電子機器による記録または再生に利用される場合に、その記憶媒体上の前記コントローラにて当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記リボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、

無効化すべきでないと判定した場合だけ、前記記憶媒体上のコントローラから前記電子機器に対して当該記憶媒体に固有の秘匿されたメディア識別情報を渡し、前記電子機器では前記メディア識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いることを特徴とするコンテンツ管理方法。

【請求項6】 前記記憶媒体のコントローラと前記電子機器との間で、前記電子機器を表す情報、前記メディア識別情報の授受を行う際には、その都度前記コントローラと前記電子機器との間で所定のアルゴリズムに従うキー交換を行って認証鍵を共有し、前記電子機器を表す情報、前記メディア識別情報の送り側では、当該情報を自身の有する前記認証鍵で暗号化して送り、受け側では、暗号化された情報を自身の有する前記認証鍵で復号して使用することを特徴とする請求項5記載のコンテンツ管理方法。

【請求項7】 配信する暗号化デジタルコンテンツ、または記憶媒体に記録された暗号化デジタルコンテンツに、コンテンツ保護のために無効化すべき、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器が判別可能なリボケーション情報を付加し、

前記暗号化デジタルコンテンツを、記憶メディア部とコントローラとが一体化された記憶媒体に電子機器により記録する際には、その記憶媒体上の前記コントローラにて当該電子機器から当該電子機器を表す情報と前記リボケーション情報が付加された暗号化デジタルコンテンツを受け取って、その受け取った電子機器を表す情報により前記リボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、

無効化すべきでないと判定した場合だけ前記暗号化デジタルコンテンツを前記記憶媒体に記録することを特徴とするコンテンツ管理方法。

【請求項8】 前記リボケーション情報に予めバージョン情報を付す一方、最新のリボケーション情報を前記記憶媒体の特定記憶領域に記憶せしめ、前記暗号化デジタルコンテンツを、前記記憶媒体に前記電子機器により記録する際には、当該コンテンツに付加されているリボケーション情報のバージョン情報と、前記特定記憶領域に記憶されているリボケーション情報のバージョン情報とを比較して、その比較結果に基づいて最新のリボケーション情報が前記特定記憶領域に記憶されるように制御し、

前記特定記憶領域に記憶されている最新のリボケーション情報を用いて前記電子機器を無効化すべきか否かの判定を行うことを特徴とする請求項7記載のコンテンツ管理方法。

【請求項9】 前記暗号化デジタルコンテンツに付加される前記リボケーション情報は、当該コンテンツを復号するためのコンテンツキーと合わせて、システムに共通のマスタキーにより暗号化されており、

前記記憶媒体に記録された暗号化デジタルコンテンツを電子機器により利用する際には、その記憶媒体上の前記コントローラにて当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記特定領域に記憶されているリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、

無効化すべきでないと判定した場合だけ、前記記憶媒体上のコントローラから前記電子機器に対して秘匿された前記マスタキーを渡し、

前記電子機器では前記マスタキーを前記コンテンツキーの復号化に用いることを特徴とする請求項7記載のコンテンツ管理方法。

【請求項10】 コンテンツ保護のために無効化すべき、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器が判別可能なリボケーション情報が予め登録された特定記憶領域を有する記憶メディア部とコントローラとが一体化された記憶媒体とのインタフェースを持ち、当該インタフェースを通してコンテンツの記録または再生が可能な電子機器であって、前記記憶媒体をデジタルコンテンツの記録または再生に利用するに際し、自身を表す情報を前記記憶媒体に渡すことで、当該情報により前記記憶媒体のコントローラにて前記リボケーション情報を参照させて、その参照結果に応じて前記記憶媒体に固有の秘匿されたメディア識別情報を前記コントローラから受け取る手段と、前記メディア識別情報によりコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化を行う手段とを具備することを特徴とする電子機器。

・【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像データや音楽データに代表される種々のデジタルコンテンツを記録再生するのに用いられる記憶媒体に係り、特に不当な電子機器によるコンテンツの記録再生を抑止するのに好適な、記憶媒体及び同媒体を使用したコンテンツ管理方法に関する

【0002】

【従来の技術】近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレーヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メデ

ニアに格納された画像データや音楽データなど様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。

【0003】これらのデジタルコンテンツは、例えばMP3、MP3といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。

【0004】

【発明が解決しようとする課題】しかし、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器で用いられる記憶媒体は、別の機器に移動しても記録／再生できるリバーシブルなものが多く、その仕様は基本的にはオープンである。このためコンテンツの移動／コピーを自由に行うことができるので、記憶媒体に記憶されたコンテンツを不正なコピー／移動から保護することは実際上困難である。

【0005】そこで、メモ리카ードのように記憶メディア部とコントローラとが一体化された記憶媒体については、秘匿された特定手続にてのみアクセスでき、ユーザからはアクセスできないアクセス不能領域（秘匿領域）を設け、そこにコピー制御情報、移動制御情報などの、コンテンツの使用に必要な重要な情報を格納しておくことにより、コンテンツの保護を図ることが考えられる。

【0006】この場合、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器と記憶媒体の間でコンテンツのコピー／移動を行う際には、それぞれが、著作権保護（コンテンツ保護）に関する所定の仕組み（つまり所定のコンテンツ保護機能）を共有している正当なものであるかを相互に認証し、正しいと認証できた場合に相互に共有する鍵生成のアルゴリズムに従って鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキー（コンテンツを暗号化するキー）の暗号化（ライセンス暗号化）／復号化またはコンテンツの暗号化／復号化に用いることも考えられる。

【0007】ところが、上記相互認証に必要な情報は、機器の出荷段階で予め設定されていることから、機器の購入後に当該機器（上で動作するプログラム）が改変されるといった攻撃により、例えばコンテンツ保護の仕組みが無効なものになった場合等においては、上記相互認証だけでは、この種の、問題のある機器を検出できないことになる。

【0008】しかも、上記した問題のある機器を検出する方法が考えられたとしても、相互に鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキーの暗号化／復号化またはコンテンツの暗号化／復号化に用いる方式では、この種の機器を排除できないことが予測される。その理由は、たとえ問題のある機器が検出

できたとしても、その機器と記憶媒体との間で認証鍵の交換が行われると、その認証鍵を用いてコンテンツキーの暗号化／復号化またはコンテンツの暗号化／復号化が行われるからである。

【0009】本発明は上記事情を考慮してなされたものでその目的は、無効化すべき電子機器が判別可能なリポケーション情報に基づいて問題のある機器を確実に検出して無効化すると共に、無効化しない機器の場合には、無効化されたならば利用不可能な記憶媒体に固有の識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いさせることで、不当な機器による利用を確実に防止できる記憶媒体及び同媒体を使用したコンテンツ管理方法を提供することにある。

【0010】本発明の他の目的は、リポケーション情報を常に最新なものに更新できる記憶媒体及び同媒体を使用したコンテンツ管理方法を提供することにある。

【0011】

【課題を解決するための手段】本発明の記憶媒体は、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、コンテンツ保護のために無効化すべき電子機器が判別可能なリポケーション情報が予め登録された特定記憶領域と、任意の電子機器による記録または再生に利用される場合に、当該電子機器から当該電子機器を表す情報を受け取って、その情報により上記リポケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定する判定手段と、この判定手段により無効化すべきでない判定された場合だけ、上記電子機器に対して自身に固有の秘匿されたメディア識別情報を渡して、そのメディア識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いさせる暗号化／復号化キー送出手段とを含むコントローラとを備えたことを特徴とする。

【0012】このように本発明の記憶媒体においては、その特定記憶領域にリポケーション情報が予め登録された構成とする一方、メモ리카ードのように、記憶メディア部とコントローラとが一体化された構成とし、当該記憶媒体が任意の電子機器による記録または再生に利用される場合に、上記コントローラが当該電子機器から当該電子機器を表す情報を受け取って、その情報によりリポケーション情報を参照し、その参照結果に応じて当該電子機器の無効化を制御すると共に、無効化すべきでない場合には、電子機器に対して自身に固有の秘匿されたメディア識別情報を渡して、そのメディア識別情報をコンテンツまたはコンテンツ復号用のコンテンツキーの暗号化または復号化に用いさせることにより、リポケーション情報から正当と認められる電子機器においてのみ、コンテンツまたはコンテンツキーの暗号化／復号化が可能となり、記憶媒体側で不当な電子機器によるコンテンツ

の記録または再生を確実に抑止することが可能となる。

【0013】ここで、上記特定記憶領域を、読み出し専用の不揮発性メモリ上に確保するか、或いは秘匿された特定手段以外ではアクセスできない書き換え可能な不揮発性メモリ上に確保するならば、リボケーション情報の改ざんにも対処可能となる。

【0014】また、本発明の記憶媒体は、リボケーション情報が付加されたデジタルコンテンツを扱う新規なシステムに対応可能なように、上記コントローラとして、以下の各手段、即ちリボケーション情報が付加されたデジタルコンテンツが電子機器により記録される際には、当該リボケーション情報により上記特定記憶領域上のリボケーション情報を更新する更新手段と、デジタルコンテンツが電子機器により記録される際と、本記憶媒体に記録されたデジタルコンテンツが電子機器により利用される際には、当該電子機器から当該電子機器を表す情報を受け取って、その情報により上記特定記憶領域に記憶されている最新のリボケーション情報を参照することで、その参照結果に応じて当該電子機器を無効化すべきか否かを判定し、その判定結果に応じて当該電子機器の無効化を制御する判定手段とを備えたコントローラを用いたことを特徴とする。ここで、上記特定記憶領域を、秘匿された特定手段以外ではアクセスできない書き換え可能な不揮発性メモリ上に確保するとよい。

【0015】このような構成の記憶媒体とすることで、当該記憶媒体の特定記憶領域に登録されるリボケーション情報を常に最新のものに更新することができ、不当な電子機器によるコンテンツの記録（コピー）を効果的に防止することができる。

【0016】また、デジタルコンテンツに付加されるリボケーション情報にバージョン情報が付されるシステム、即ちバージョン情報付きリボケーション情報（バージョン管理されたリボケーション情報）を扱うシステムに対処可能なように、上記更新手段に、デジタルコンテンツに付加されたりリボケーション情報のバージョン情報と上記特定記憶領域に記憶されているリボケーション情報のバージョン情報とを比較し、その比較結果に基づいて上記特定記憶領域に最新のリボケーション情報が記憶されるように更新制御する機能を持たせるならば、上記バージョン情報を有効利用して、記憶媒体の特定記憶領域に登録されるリボケーション情報を確実に最新のものに更新することができる。

【0017】また、本発明の記憶媒体は、バージョン情報付きリボケーション情報が付加された暗号化デジタルコンテンツであって、当該リボケーション情報がコンテンツ復号用のコンテンツキーと合わせてシステムに共通のマスタキーにより暗号化された暗号化デジタルコンテンツを扱う新規なシステムに対応可能なように、上記コントローラに次の手段、即ち上記判定手段により無効化すべきでないと判定された場合だけ、該当する電子機器

に対して秘匿されたマスタキーを渡して、そのマスタキーをコンテンツ復号用のコンテンツキーの復号化に用いさせるマスタキー送出手段を設けたことをも特徴とする。この構成においては、不当な電子機器によるコンテンツの利用（例えば再生）を効果的に防止することができる。

【0018】なお本発明は、上記構成の記憶媒体を使用したコンテンツ管理方法としても成立し、上記構成の記憶媒体を利用する、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器としても成立する。

【0019】

【発明の実施の形態】以下、本発明の実施の形態につき図面を参照して説明する。

【0020】図1は本発明の一実施形態に係るコンテンツ利用管理システム1の構成例を示す。なお、ここでは、コンテンツ（デジタルコンテンツ）として音楽データを一例として用いているが、この場合に限らず、映画や、ゲームソフト等のデータであってもよい。

【0021】EMD（Electronic Music Distributor）は、音楽配信サーバまたは音楽配信放送局である。

【0022】コンテンツ利用管理システム（以下、LCM（Licence（SDMI-）Compliant Module）と称する）1は、例えば、パーソナルコンピュータ（PC）を用いて実現される。このLCM1におけるコンテンツ保護の方法は、コンテンツを記録すべき記憶メディア（記憶媒体）13毎に、その記憶メディアの識別情報（メディアID）を用いてコンテンツの暗号化／復号化を管理することを前提としている。

【0023】LCM1は、複数のEMD（ここでは、EMD#1～#3）に対応した受信部#1～#3を有しており、当該受信部#1～#3を通してEMDが配信する暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツ復号キー）などを受信する。受信部#1～#3は、再生機能や課金機能を有していても良い。また、課金機能を利用して、気に入ったコンテンツを購入することが可能である。

【0024】LCM1は、セキュア・コンテンツ・サーバ（ここでは、Secure Music Server：SMSであり、以下SMSと称する）2を有する。このSMS2は、利用者が購入した暗号化コンテンツをEMD1/F（インタフェース）部3を経由して受け取る。暗号化コンテンツ（ここでは音楽コンテンツ）は、必要に応じてEMD1/F部3で復号され、形式変換や再暗号化が施される。SMS2は暗号化コンテンツを受け取ると、それを音楽データ格納部10に格納し、音楽データ復号鍵（コンテンツ復号キー）をライセンス格納部9に格納する。ここでSMS2は、配信された音楽コンテンツを利用者が試聴するために再生機能を有していても良く、この場合、SMS2が管理する音楽コンテンツをPC上で再生

することができる。

【0025】SMS2はまた、メディア1/F部6に装着可能なメモ리카ード等の記憶メディア（以下、PM（Portable Memory）と称する）13に対してコンテンツデータ（デジタルコンテンツ）を当該1/F部6経由で出力する機能を有している。このPM13は、図2に示す構成の専用の記録再生装置（以下、簡単にPD（Portable Device）と称する）12にセットして用いることで、当該PM13に記録されたコンテンツをPD12上で再生することができる。

【0026】SMS2からPM13へのコンテンツの記録は、メディア1/F部6を通じて直接行われるか、またはPD12を経由して行うことができる。

【0027】ここで、LCM1によるチェックイン/チェックアウト機能について簡単に説明する。チェックアウトとは、LMS1が「親」としてのコンテンツを格納しており、PM13に、その複製を「子」コンテンツとしてコピーすることをいう。「子」コンテンツは基本的にはPD12で自由に再生することが可能であるが、

「子」から「孫」コンテンツを作成することは許されない。「親」が幾つ「子」を生むことができるかは、

「親」の属性として定義される。また、チェックインとは、例えば、PM13をLCM1のメディア1/F部6に装着し、LCM1が「子」コンテンツを消去（または利用不能）することで、LCM1内の「親」コンテンツは「子」を1つ作る権利を回復することをいう。これを「親」にチェックインするともいう。

【0028】PM13は、図3に示すように、コントローラ130と、公開領域131及び秘匿領域134からなる記憶メディア部とから構成される。秘匿領域134は、コントローラ130を通して非公開の手順（つまり秘匿された特定手続）でしかアクセスできない記憶領域であり、コンテンツ復号に必要な情報を記憶するのに用いられる。秘匿領域134は、対応するPM13に固有のメディア識別情報（以下、メディアキーと称する） K_M 等の定数が記憶される秘匿ROM領域と、ライセンスする側から提供される（メディアマークと呼ばれる）秘密データであるライセンス復号キー等の変数が記憶される秘匿R/W（リード/ライト）領域からなる。メディアキー K_M は、各PM13に固有であればよく、シリアル番号や製造番号（PM13個々の製造番号、または製造ロット番号）、他の様々な識別情報を用いることができる。なお、メディアキー K_M を、各PM13に固有な識別情報とライセンス復号キーから生成するようにしても構わない。秘匿ROM領域は例えばROM（読み出し専用の不揮発性メモリ）上に確保され、秘匿R/W領域は例えばフラッシュメモリ（書き換え可能な不揮発性メモリ）の特定領域に確保される。

【0029】公開領域131は、秘匿領域以外の、通常の手順にてアクセス可能な領域であり、読み出し専用の

公開領域（以下、公開ROM領域と称する）132と、書き換え可能な公開領域（以下、公開R/W領域と称する）133からなる。公開ROM領域は例えばROM上に確保され、公開R/W領域は例えばフラッシュメモリ上に確保される。この公開ROM領域、公開R/W領域は、先の秘匿ROM領域が確保されるROM、秘匿R/W領域が確保されるフラッシュメモリ上に、それぞれ確保されるようにしても構わない。

【0030】公開ROM領域132には、本発明に直接関係するリボケーション情報が対応するPM13の出荷段階で予め登録されている。このリボケーション情報は、コンテンツの保護のためにPM13の利用を無効化すべき機器（LCM、PD）、更に具体的に述べるならばPM13（内の公開R/W領域133）を対象とするデジタルコンテンツの記録または再生のためのアクセス要求を無効化すべき機器（LCM、PD）が判別可能な情報である。本実施形態において、リボケーション情報は無効化すべき機器の識別情報（デバイスID）のリストである。そこで、以下の説明では、「リボケーション情報」に代えて「リボケーションリストRL」なる用語を用いる。つまり、公開ROM領域132には、リボケーションリストRLが予め登録されている。

【0031】公開R/W領域133には、暗号化されたコンテンツキー（コンテンツ復号キー）、暗号化されたコンテンツ等が適宜記憶される。暗号化されたコンテンツキーは、コンテンツCを復号するための（当該コンテンツCに固有の）コンテンツキー K_C を、PM13に依存するメディアキー K_M で暗号化することで取得されるものである。また、暗号化されたコンテンツ（ここでは2重に暗号化されたコンテンツ）は、 K_C で暗号化されたコンテンツ（ $K_C[C]$ ）をPM13に依存するメディアキー K_M で暗号化する（ $K_M[K_C[C]]$ ）ことで取得されるものである。

【0032】LCM1、PD12もまた、図4に示すようにPM13と同様の記憶領域を有している。即ちLCM1は、公開ROM領域112及び公開R/W領域113からなる公開領域111と、非公開の手順でしかアクセスできない秘匿領域114との各記憶領域を有している。公開R/W領域113には、図1に示す音楽データ格納部10が確保されている。秘匿領域114には、LCM1の識別情報（デバイスID） ID_{LCM} が予め記憶されている。秘匿領域114にはまた、各コンテンツ毎のコンテンツキー K_C が適宜記憶される。秘匿領域114には更に、図1に示す宿帳格納部8が確保されている。SMS2の管理下にある音楽データ格納部10（公開R/W領域113）にて保持される全ての音楽コンテンツは、その識別情報であるコンテンツID（TID）と予め定められた複製可能コンテンツ数、即ち子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼び、（秘匿領域114内の）宿

帳格納部8に格納される。LCM1は、SMS2にてこの宿帳格納部8にアクセスするための秘匿された特定の手段が行われた後、宿帳格納部8（を提供する秘匿領域114）からデータを読み取るための秘匿領域ドライバ7を有している。なお、この宿帳は本発明に直接関係しないため、その利用方法の詳細については説明を省略する。

【0033】一方、PD12は、公開ROM領域122及び公開R/W領域123からなる公開領域121と、非公開の手順でしかアクセスできない秘匿領域124と各記憶領域を有している。秘匿領域124には、PD12の識別情報ID_{PD}が予め固定記憶されている。秘匿領域124にはまた、各コンテンツ毎のコンテンツキーK_Cが適宜記憶される。

【0034】図2は、PD12の構成例を示す。PM13は、PD12のメディアI/F部12fに装着して利用される。LCM1がPD12を介してPM13に読み書きする場合は、LCM1内のPDI/F部5、PD12内のLCM-I/F部12e、メディアI/F部12fを経由して当該PM13の秘匿領域134（図3参照）にアクセスする。メディアI/F部12fは、PM13の秘匿領域134にアクセスするための秘匿領域アクセス部（図示せず）を有している。PD12内の公開R/W領域123及び秘匿領域124（図4参照）は、例えばフラッシュメモリ12d上に確保されている。また公開ROM領域122（図4参照）は、ROM12c上に確保されている。このROM12cには、PM13との間で相互認証を行うためのプログラムが書き込まれている。PD12では、CPU12aの制御のもと、このプログラムに従ってPM13との間の相互認証等の処理が実行される。

【0035】次に、本実施形態の動作について、EMDから配信された暗号化された音楽コンテンツをLCM1のEMDI/F部3で受信して、SMS2により音楽データ格納部10に一時格納した後、その「複製」を「子」コンテンツとして、例えばメディアI/F部6に装着されたPM13に記録（コピー）するチェックアウト時の動作を例に、図5の流れ図を参照して説明する。

【0036】この場合、チェックアウトの指示が例えばLCM1のユーザI/F部15を介してなされ、且つPM13がLCM1のメディアI/F部6に装着された段階で、LCM1のメディアI/F部6とPM13のコントローラ130との間で周知の相互認証が行われる（ステップS101）。この相互認証は、LCM1を機器A、PM13を機器Bとすると、次のように行われるのが一般的である。

【0037】まず、機器Aから機器Bを認証するものとする。ここで機器Aは、公開鍵k_pを保持しており、機器Bは、機器Aとの間で所定のコンテンツ保護機能を共有しているならば、公開鍵k_pに対応する秘密鍵k_sを

保持している。機器Aは乱数Rを発生して機器Bに送る。機器Bは、機器Aで発生された乱数Rを受け取ると、それを秘密鍵k_sで暗号化して、その暗号化された乱数(k_s[R]と表す)を機器Aに返す。機器Aでは、公開鍵k_pを用いて、k_s[R]を復号し、復号結果が先に発生した乱数Rに等しければ、機器Bは正しい相手であると判定する。

【0038】その後、上記と同じことを機器Bから機器Aに対して行うことで、相互認証を行うことができる。

10 この場合、機器Bは公開鍵を保持し、機器Aは秘密鍵を保持し、機器Aが機器Bにて発生した乱数を秘密鍵で暗号化してそれを機器Bで公開鍵を用いて復号し、先に発生した乱数に等しいかを確認する。

【0039】以上の相互認証(S101)により、LCM1及びPM13の双方にて正当な相手であることが確認されたとき、LCM1のメディアI/F部6とPM13のコントローラ130との間でキー交換が行われ、同一の認証鍵(K_{X1})が共有される。このキー交換は、例えばDVD-ROMのコンテンツ暗号化アルゴリズムとして使用されているCSS(Content Scrambling System)に代表されるランダムチャレンジ・レスポンスを用いた方法により行われる。認証鍵(K_{X1})は毎回代わる時変キーである。

【0040】LCM1のメディアI/F部6は、秘匿領域114に秘匿（記憶）されている自身の識別情報ID_{LCM}を読み出して当該ID_{LCM}を認証鍵(K_{X1})で暗号化し、その暗号化されたID_{LCM}(=K_{X1}[ID_{LCM}])をメディアI/F部6からPM13に送る（ステップS102）。

30 【0041】PM13のコントローラ130は、LCM1側からのK_{X1}[ID_{LCM}]を、先のキー交換で取得した認証鍵(K_{X1})で復号し、ID_{LCM}を得る（ステップS103）。次にPM13のコントローラ130は、復号したLCM1の識別情報ID_{LCM}により公開ROM領域132内のリボケーションリストRLを参照し、当該ID_{LCM}に一致する識別情報が登録されているか否かにより、LCM1によるPM13の利用を無効化するか否かを判定する（ステップS104）。

40 【0042】もし、ID_{LCM}に一致する識別情報がリボケーションリストRLに登録されている場合には、コントローラ130は該当するLCM1によるPM13の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【0043】これに対し、ID_{LCM}に一致する識別情報がリボケーションリストRLに登録されていない場合は、コントローラ130は該当するLCM1によるPM13の利用が許可されているものと判定し、秘匿領域134に秘匿されているメディアキーK_Mを読み出し出力する（ステップS105）。そしてコントローラ130は、LCM1のメディアI/F部6との間で（当該LC

M1のメディア1/F部6を介して) キー交換を行い、同一の認証鍵(K_{x2})を共有した上で、上記読み出したメディアキー K_M を認証鍵(K_{x2})で暗号化し、その暗号化された $K_M (=K_{x2} [K_M])$ をLCM1に送る(ステップS106)。

【0044】LCM1のメディア1/F部6は、PM13側からの $K_{x2} [K_M]$ を、先のキー交換で取得した認証鍵(K_{x2})で復号し、メディアキー K_M を得る(ステップS107)。次にLCM1のメディア1/F部6は、秘匿領域114に秘匿されているコンテンツキー K_C を取得したメディアキー K_M により暗号化し、その暗号化された $K_C (=K_M [K_C])$ をPM13の公開R/W領域133に書き込む(ステップS108)。

【0045】このように本実施形態では、リボケーションリストRLに従って無効化(リボケート)されたならばPM13から渡されることのない(暗号化された)メディアキー K_M を、当該PM13からLCM1が受け取って、そのLCM1の秘匿領域114に秘匿されているコンテンツキー K_C を当該メディアキー K_M により暗号化して、PM13の公開R/W領域133に書き込むようにしている。このため、LCM1とPM13との間で認証鍵の交換を行い、その認証鍵を用いてコンテンツキーの暗号化/復号化を行う方法に比べて、リボケーションリストRLで指定される無効化対象LCM(PM13を利用しようとする電子機器)を確実に無効化(排除)できる。なお、LCM1の公開R/W領域113に確保された音楽データ格納部10に蓄積されている暗号化コンテンツ($K_C [C]$)をPM13に送る際に、上記取得した K_M で更に暗号化するようにしても構わない。

【0046】次に、PM13に格納された暗号化コンテンツをPD12上で復号して再生する場合の動作について、図6の流れ図を参照して説明する。まず、再生の指示が例えばPD12に対してなされ、且つPM13がPD12のメディア1/F部12fに装着された段階で、PD12のCPU12aとPM13のコントローラ130との間で(前記ステップS101と同様の)相互認証が行われる(ステップS201)。そして、この相互認証(S201)により、PD12及びPM13の双方にて正当な相手であることが確認されたとき、PD12のCPU12aとPM13のコントローラ130との間でキー交換が行われ、同一の認証鍵(K_{x3})が共有される。

【0047】PD12のCPU12aは、秘匿領域124に秘匿されている自身の識別情報 ID_{PD} を読み出して当該 ID_{PD} を認証鍵(K_{x3})で暗号化し、その暗号化された $ID_{PD} (=K_{x3} [ID_{PD}])$ をメディア1/F部12fからPM13に送る(ステップS202)。

【0048】PM13のコントローラ130は、PD12側からの $K_{x3} [ID_{PD}]$ を、先のキー交換で取得した認証鍵(K_{x3})で復号し、 ID_{PD} を得る(ステップS

03)。次にPM13のコントローラ130は、復号したPD12の識別情報 ID_{PD} により公開ROM領域132内のリボケーションリストRLを参照し、当該 ID_{PD} に一致する識別情報が登録されているか否かにより、PD12によるPM13の利用を無効化するか否かを判定する(ステップS204)。

【0049】もし、 ID_{PD} に一致する識別情報がリボケーションリストRLに登録されている場合には、コントローラ130は該当するPD12によるPM13の利用を無効化(リボケート)すべきものと判定し、以降の処理を停止する。

【0050】これに対し、 ID_{PD} に一致する識別情報がリボケーションリストRLに登録されていない場合は、コントローラ130は該当するPD12によるPM13の利用が許可されているものと判定し、秘匿領域134に秘匿されているメディアキー K_M を読み出し出力する(ステップS205)。そしてコントローラ130は、PD12のCPU12aとの間で(当該PD12のメディア1/F部12fを介して)キー交換を行い、同一の認証鍵(K_{x4})を共有した上で、上記読み出したメディアキー K_M を認証鍵(K_{x4})で暗号化し、その暗号化された $K_M (=K_{x4} [K_M])$ をPD12に送る(ステップS206)。

【0051】PD12のCPU12aは、PM13側からの $K_{x4} [K_M]$ を、先のキー交換で取得した認証鍵(K_{x4})で復号し、メディアキー K_M を得る(ステップS207)。次にPD12のCPU12aは、PM13の公開R/W領域133に記憶されている暗号化されたコンテンツキー $K_C (=K_M [K_C])$ を読み込んで、ステップS207で取得したメディアキー K_M により復号し、その復号されたコンテンツキー K_C を秘匿領域124に書き込んで秘匿化する(ステップS208)。したがってPD12では、この復号されたコンテンツキー K_C (と、必要ならば先に復号化したメディアキー K_M と)を利用して、PM13の公開R/W領域133に記憶されている暗号化コンテンツを復号して再生することが可能となる。

【0052】このように本実施形態では、リボケーションリストRLに従って無効化(リボケート)されたならばPM13から渡されることのない(暗号化された)メディアキー K_M を、当該PM13からPD12が受け取って、当該PM13の秘匿領域134に秘匿されている暗号化コンテンツキー($K_M [K_C]$)を、そのメディアキー K_M により復号化して、PD12の秘匿領域124に書き込むようにしている。このため、PD12とPM13との間で認証鍵の交換を行い、その認証鍵を用いて暗号化コンテンツキーの復号化を行うのに比べて、リボケーションリストRLで指定される無効化対象PD(PM13を利用しようとする電子機器)を確実に無効化できる。

【0053】なお、以上の実施形態では、LCM1とPM13の間、PD12とPM13の間で、秘匿領域に秘匿されている情報、または秘匿領域に秘匿すべき情報の授受を行う際に、当該情報を認証鍵(K_{xs})により暗号化するものとしたが、認証鍵による暗号化は必ずしも必要ではない。但し、コンテンツ保護をより確実なものとするには、認証鍵による暗号化を行うことが好ましい。

【0054】また、以上の実施形態では、リボケーションリストRLが公開ROM領域132に登録されているものとして説明したが、リボケーションリストRLが改ざんされない領域であれば良く、例えば秘匿された特定手続でしかアクセスできない秘匿領域134に登録されるようにしても良い。

【0055】また、以上に述べた実施形態では、各PM13(の公開R/W領域133)に予めリボケーションリストRLが登録されているものとして説明したが、これに限るものではない。例えば、コンテンツ毎にリボケーションリストRLを付加するようにしてもよい。この場合、システムに共通の秘密キー(以下、マスターキーと称する) K_m を用意し、EMBにより配信されるコンテンツであれば、当該コンテンツをコンテンツキー K_c により暗号化して配信する際に、そのコンテンツキー K_c とリボケーションリストRLをまとめてマスターキー K_m により暗号化して($K_m[K_c+RL]$ と表す)送ればよい。また、CD(コンパクトディスク)等の記憶媒体に予め記憶されるコンテンツ(暗号化コンテンツ)であれば、そのコンテンツの復号キー、つまりコンテンツキー K_c にリボケーションリストRLを付加し、両者をまとめてマスターキー K_m により暗号化して記憶すればよい。なお、マスターキー K_m はPM13の秘匿領域134に予め格納されているものとする。

【0056】以下、コンテンツ毎にリボケーションリストRLを有する場合の動作を説明する。なお、リボケーションリストRLには、バージョン情報が付されているものとする。

【0057】まず、EMDから配信された、リボケーションリストRL付きの暗号化された音楽コンテンツをLCM1のEMD1/F部3で受信して、SMS2により音楽データ格納部10に一時格納した後、その「複製」を「子」コンテンツとして、例えばメディア1/F部6に装着されたPM13に記録(コピー)するチェックアウト時の動作を例に、図7の流れ図を参照して説明する。

【0058】この場合、チェックアウトの指示が例えばLCM1のユーザ1/F部15を介してなされ、且つPM13がLCM1のメディア1/F部6に装着された段階で、LCM1のメディア1/F部6とPM13のコントローラ130との間で相互認証が行われる(ステップS301)。

【0059】この相互認証(S301)により、LCM

1及びPM13の双方にて正当な相手であることが確認されると、LCM1のメディア1/F部6は、 $K_m[K_c+RL]$ 、 $K_c[C]$ をPM13の公開R/W領域133に記憶する(ステップS302、S303)。このとき、LCM1のメディア1/F部6とPM13のコントローラ130との間でキー交換が行われ、同一の認証鍵(K_{xs})が共有される。

【0060】PM13のコントローラ130は、公開R/W領域133に記憶されている $K_m[K_c+RL]$ を、秘匿領域134に秘匿されているマスターキー K_m により復号し、 K_c+RL を得る(ステップS304)。

【0061】次にコントローラ130は、 K_c+RL からコンテンツキー K_c に付加されているリボケーションリストRLを抽出して、当該RLのバージョン情報と秘匿領域134に秘匿されている現リボケーションリストRLのバージョン情報とを比較し、抽出したリボケーションリストRLの方が新しいバージョン情報である場合に、秘匿領域134内の現リボケーションリストRLを、抽出したリボケーションリストRLに更新する(ステップS305)。これにより、秘匿領域134内のリボケーションリストRLが最新のものに更新される。なお、秘匿領域134にリボケーションリストRLが秘匿されていない場合には、抽出したリボケーションリストRLをそのまま秘匿領域134に登録する。

【0062】さて、相互認証(S301)により、LCM1及びPM13の双方にて正当な相手であることが確認された場合、LCM1のメディア1/F部6は、秘匿領域114に秘匿されている自身の識別情報 ID_{LCM} を読み出して当該 ID_{LCM} を上記認証鍵(K_{xs})で暗号化し、その暗号化された ID_{LCM} (= $K_{xs}[ID_{LCM}]$)をメディア1/F部6からPM13に送る(ステップS306)。

【0063】PM13のコントローラ130は、LCM1側からの $K_{xs}[ID_{LCM}]$ を、先のキー交換で取得した認証鍵(K_{xs})で復号し、 ID_{LCM} を得る(ステップS307)。次にPM13のコントローラ130は、ステップS305でのリボケーションリストRL更新の有無を確認した後、復号したLCM1の識別情報 ID_{LCM} により秘匿領域134内の最新のリボケーションリストRLを参照し、当該 ID_{LCM} に一致する識別情報が登録されているか否かにより、LCM1によるPM13の利用を無効化するか否かを判定する(ステップS308)。

【0064】もし、 ID_{LCM} に一致する識別情報がリボケーションリストRLに登録されている場合には、コントローラ130は該当するLCM1によるPM13の利用を無効化すべきものと判定し、公開R/W領域133に記憶された $K_m[K_c+RL]$ 、 $K_c[C]$ を消去して(または無効化して)、以降の処理を停止する。

【0065】これに対し、 ID_{LCM} に一致する識別情報

がリボケーションリストRLに登録されていない場合は、コントローラ130は該当するLCM1によるPM13の利用が許可されているものと判定し、キーの受け渡し等、以降の処理を継続する。

【0066】以上の動作は、CD（コンパクトディスク）をLCM1のCD1/F部11に装着して、当該CDに予め記憶されているリボケーションリストRL付きの暗号化された音楽コンテンツをSMS2により音楽データ格納部10に一時格納した後、その「複製」を「子」コンテンツとして、例えばメディア1/F部6に装着されたPM13に記録（コピー）する場合についても同様である。

【0067】次に、PM13（の公開R/W領域133）に格納された暗号化コンテンツをPD12上で復号して再生する場合の動作について、図8の流れ図を参照して説明する。まず、再生の指示が例えばPD12に対してなされ、且つPM13がPD12のメディア1/F部12fに装着された段階で、PD12のCPU12aとPM13のコントローラ130との間で相互認証が行われる（ステップS401）。そして、この相互認証（S401）により、PD12及びPM13の双方にて正当な相手であることが確認されたとき、PD12のCPU12aとPM13のコントローラ130との間でキー交換が行われ、同一の認証鍵（ K_{x6} ）が共有される。

【0068】PD12のCPU12aは、秘匿領域124に秘匿されている自身の識別情報ID_{PD}を読み出して当該ID_{PD}を認証鍵（ K_{x6} ）で暗号化し、その暗号化されたID_{PD}（ $=K_{x6}[ID_{PD}]$ ）をメディア1/F部12fからPM13に送る（ステップS402）。

【0069】PM13のコントローラ130は、PD12側からの $K_{x5}[ID_{PD}]$ を、先のキー交換で取得した認証鍵（ K_{x6} ）で復号し、ID_{PD}を得る（ステップS403）。次にPM13のコントローラ130は、復号したPD12の識別情報ID_{PD}により秘匿領域134内のリボケーションリストRLを参照し、当該ID_{PD}に一致する識別情報が登録されているか否かにより、PD12によるPM13の利用を無効化するか否かを判定する（ステップS404）。

【0070】もし、ID_{PD}に一致する識別情報がリボケーションリストRLに登録されている場合には、コントローラ130は該当するPD12によるPM13の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【0071】これに対し、ID_{PD}に一致する識別情報がリボケーションリストRLに登録されていない場合は、コントローラ130は該当するPD12によるPM13の利用が許可されているものと判定し、秘匿領域134に秘匿されているマスターキー K_m を読み出し出力する（ステップS405）。そしてコントローラ130は、PD12のCPU12aとの間で（当該PD12のメディア

1/F部12fを介して）キー交換を行い、同一の認証鍵（ K_{x7} ）を共有した上で、上記読み出したマスターキー K_m を認証鍵（ K_{x7} ）で暗号化し、その暗号化された K_m （ $=K_{x7}[K_m]$ ）をPD12に送る（ステップS406）。

【0072】PD12のCPU12aは、PM13側からの $K_{x7}[K_m]$ を、先のキー交換で取得した認証鍵（ K_{x7} ）で復号し、マスターキー K_m を得る（ステップS407）。次にPD12のCPU12aは、PM13の公開R/W領域133に記憶されている $K_m[K_c+RL]$ を読み込んで、ステップS407で取得したマスターキー K_m により復号し、その復号された K_c+RL からコンテンツキー K_c を抽出する（ステップS408）。なお、復号された K_c+RL から K_c とRLを抽出するには、例えば K_c とRLに所定のヘッダ情報を持たせ、当該ヘッダ情報を検出すればよい。

【0073】そしてCPU12aは、PM13の公開R/W領域133に記憶されている暗号化コンテンツ（ $K_c[C]$ ）を読み込んで、ステップS408で取得したコンテンツキー K_c により復号し、コンテンツCを得る（ステップS409）。これによりPD12でのコンテンツの再生が可能となる。

【0074】このように本実施形態では、EMBから配信された、またはCDに記録されたコンテンツをLCM1によりPM13に記録する際に、当該コンテンツに付加されたリボケーションリストRLに応じて秘匿領域134内のリボケーションリストRLが最新のものとなるように制御している。このため、各PM13毎にリボケーションリストRLを用意する場合に比べて、最新のリボケーションリストRLに従って、LCM1によるPM13の利用を無効化することができる。また、PM13に記録された暗号化コンテンツをPD12上で再生する際には、リボケーションリストRLに従って無効化されたならばPM13から渡されることのない（暗号化された）マスターキー K_m を、当該PM13からPD12が受け取って、 $K_m[K_c+RL]$ からコンテンツキー K_c を復号し、そのコンテンツキー K_c により $K_c[C]$ からコンテンツを復号するようにしたので、無効化対象PD12（PM13を利用しようとする電子機器）を確実に無効化できる。

【0075】

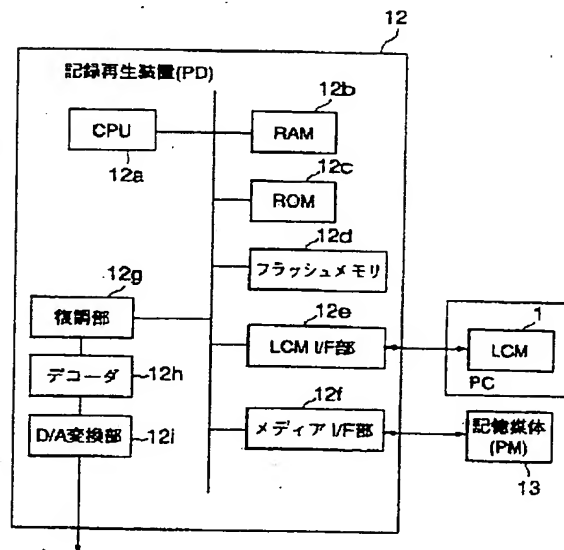
【発明の効果】以上詳述したように本発明によれば、リボケーション情報に従って問題のある機器を検出して記憶媒体の利用を無効化すると共に、無効化しない機器の場合には、無効化されたならば利用不可能な記憶媒体に固有の識別情報をコンテンツまたはコンテンツキーの暗号化または復号化に用いさせることができるため、不当な機器による利用を確実に防止できる。

【0076】また本発明によれば、リボケーション情報をコンテンツに付加して扱う新規なシステムにより、記

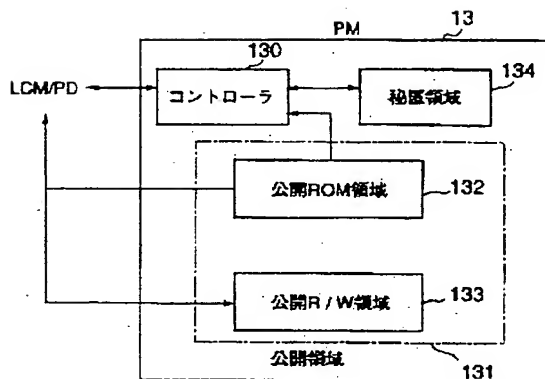
【図 7】コンテンツ毎にリポケーションリスト RL を有する場合の LCM1 から PM13 へのコンテンツ記録時

- 1…LCM (コンテンツ利用管理システム)
- 2…SMS (セキュア・コンテンツ・サーバ)
- 5…PDI / F部
- 6…メディアI / F部
- 7…秘匿領域ドライバ
- 8…宿帳格納部
- 9…ライセンス格納部
- 10…音楽データ格納部
- 11…CDI / F部
- 12…PD (記録再生装置)
- 13…PM (記憶媒体、記憶メディア)
- 112, 122, 132…公開ROM領域
- 113, 123, 133…公開R/W領域
- 114, 124, 134…秘匿領域
- 130…コントローラ

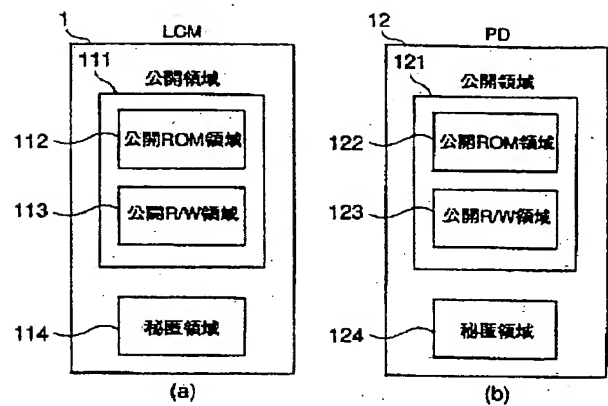
【図2】



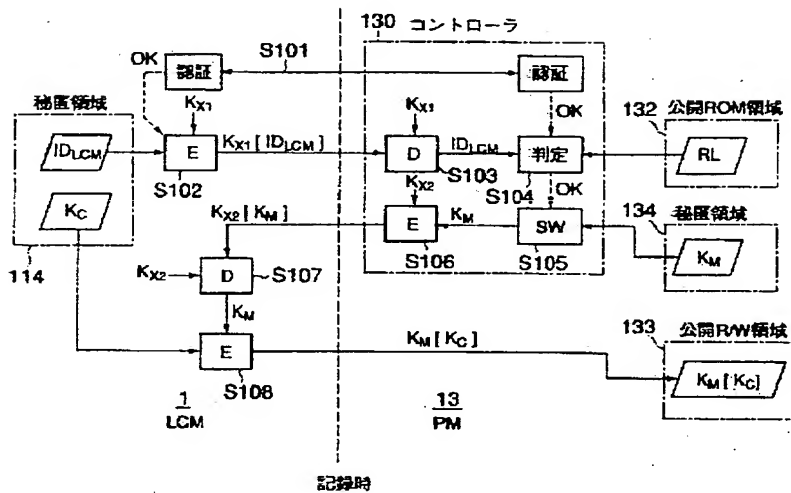
【図 3】



【圖 4】



【図5】



【图6】

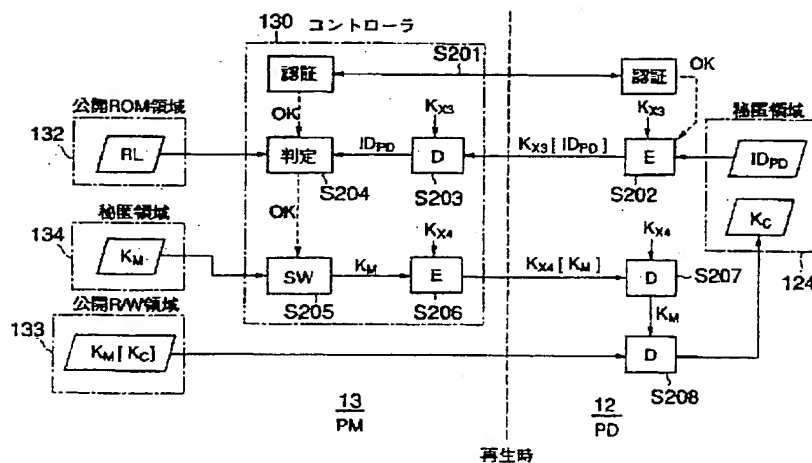


Figure 1 is a block diagram of the control system for the LCM/PM. The diagram is divided into three main sections: 114 (Secret Key Area), 130 (Controller), and 133 (Public R/W Area). Section 114 contains a box labeled ID_{LCM} . Section 130 contains several processing blocks: S301 (Verification), S306 (Encryption), S307 (Decryption), S308 (Judgment), S304 (Decryption), S305 (Update), and S303 (Key Generation). Section 133 contains two boxes: $K_m [K_C + RL]$ and $K_C [C]$. The flow starts with ID_{LCM} being encrypted by S306 using K_{XS} to produce $K_{XS}[ID_{LCM}]$. This is then decrypted by S307. S308 judges the result; if OK, it proceeds to S304, which decrypts the result using $K_C + RL$. The result is then updated by S305. The final result is stored in $K_m [K_C + RL]$ in section 133. The diagram also shows a feedback loop from S308 to S301 and S306. The diagram is labeled with "1 LCM" and "12 PM" at the bottom.

Figure 1 is a block diagram of a cryptographic system. The system is divided into three main sections: 13 (PM) and 12 (PD) on the left, and 130 (コントローラ) in the center.

Section 13 (PM):

- 秘密領域 (Secret Area):** Contains blocks RL and K_m .
- 公開R/W領域 (Public R/W Area):** Contains blocks $K_m[KC+RL]$ and $Kc[C]$.

Section 12 (PD):

- 秘密領域 (Secret Area):** Contains block $IDPD$.

Section 130 (コントローラ):

- 認証 (Authentication):** Receives $IDPD$ from the PD secret area and outputs OK to the decision block.
- 判定 (Decision):** Receives OK from authentication and RL from the PM secret area. It outputs OK to the SW block and $IDPD$ to block D (S403).
- SW (Switch):** Receives OK from the decision block and K_m from the PM secret area. It outputs K_m to block E (S406).
- Block D (S403):** Receives $IDPD$ from the decision block and K_{X6} from block E (S402). It outputs $K_{X6}[IDPD]$ to block E (S402).
- Block E (S402):** Receives K_{X6} from block D (S403) and $K_{X6}[IDPD]$ from block D (S403). It outputs OK to the authentication block.
- Block D (S407):** Receives K_{X7} from block E (S406) and K_m from the PM secret area. It outputs K_m to block D (S408).
- Block D (S408):** Receives K_m from block D (S407) and $K_m[KC+RL]$ from the PM public R/W area. It outputs Kc to block D (S409).
- Block D (S409):** Receives Kc from block D (S408) and $Kc[C]$ from the PM public R/W area. It outputs C to the PD secret area.

東京都青梅市末広町 2 丁目 9 番地 株式会
社東芝青梅工場内

Fターム(参考) 5B017 AA07 BA07 CA15